CET3529 Syllabus Fall 2009

PROFESSOR

Dr. Philip Craiger, CISSP
Department of Engineering Technology &
Assistant Director for Digital Evidence
National Center for Forensic Science
Email: WebCourses

Office: ENG 1 246 & Partnership 1 225L
Voice: 823.3527
Office hours by appointment only

COURSE DESCRIPTION

In this course the student will learn how a system administrator fulfills various organizational information resource management requirements using a Linux-based operating system. Topics will include; installation; creating and maintaining file systems; user and group administration; backup and restore processes; network configuration; various system services; simple security administration; and updating and maintaining the system.

COURSE DELIVERY

Course is a remote delivery mode that includes video and audio. It's available in a downloadable (compressed, zipped) file. Uncompress the file creates a directory with the same name as the compressed file. Go to that directory and clink on the 'index.htm' file. That will bring up your browser and video will play within it. Note the format is Flash, so you must have Flash Player installed in order to view the videos. (Google for 'flash player', and the first link should be the one to download Flash Player).

The videos vary from 20-50 minutes long. (Any longer than that and I lose your attention!). I am big on demonstrating what I'm talking about, so generally I'll discuss a topic using PowerPoint slides, and then move on over to a window that has Linux running in it (see under Course Equipment how I do this), and then demonstrate what I've discussed. It's important you follow along and attempt to replicate what I do.)

COURSE OUTCOMES

After taking this course students will be able to:

- Demonstrating an understand of the issues facing a systems administrator
- Find and draw upon resources available to a systems administrator
- Install and maintain a Linux-based computer system
- Configure networking, services and basic security on a Linux server
- Troubleshoot systems administration and network problems

CET3529 Syllabus Fall 2009

TEXTBOOK

RUTE Linux User's Manual, it's free! And good! Download it (in PDF) from the course website.

CONTENT AND ORGANIZATION

1 1 Linux Overview
1 2 Linux System Installation.
1 3 Files, Directories, and File systems
1 4 Utilities & Shells
1 5 GUIs
1 6 Networking
1 7 Introduction to Systems Administration with Linux
1 8 Installing Software

COMMUNICATIONS

There are two discussion groups, one for general discussion (you can discuss any topic with other students). There is also an 'Ask the Professor' discussion group that should be limited to questions regarding the course or a related forensic topic. Use this latter group judiciously regarding class-related questions. If you have a question about the class odds are another student has the SAME question. Please don't make me answer the same question multiple times via individual emails to students, when it would be much more efficient to do it once on the discussion group.

All class-related email communications to me MUST be through WebCourses email. If you have something urgent, you may use my regular email or call me at the number at the top of this document.

EVALUATION

There are two homework exercises and two tests. The 1st homework will be around midterm, followed by your test. Your final homework will be due a couple of weeks before finals week, and your test right after that.

COURSE EQUIPMENT

If you already have access to a running Linux system then you are set. For those of you who don't I suggest downloading VMWare player (http://www.vmware.com/products/player/) and downloading the Ubuntu desktop appliance from the Webcourses website.

I've created a how-to video that you can download and view to get your started using VMWare player. Download and view, follow instructions.

CET3529 Syllabus Fall 2009

ASSIGNMENTS

Unless otherwise stated, assignments are individual assignments, not group work. Unless otherwise stated, all assignments are due no later than 11:55PM (Eastern) on the due date.

Every assignment must be named in the following format:

<first name>.<last name>.<assignment number>.[txt,doc] (whichever extension I request)

Failure to follow this rule will result in a 25% reduction in your grade (that is, you start off with a 75).

You may post a general question to the General Discussion group if you have a question. But before you do that, try to figure out the assignment by applying what I've taught you.

ETHICS

If you cheat on an exam or homework assignment you will receive a 0 for that homework/assignment.

Plagiarizing someone's work will in an F for the course. If you are unsure of the meaning of plagiarism, I suggest you read:

http://www.uwc.ucf.edu/Writing%20Resources/Handouts/avoiding_plagiarism.htm

If you use someone else's words, then reference where you obtained the information. There is nothing wrong in doing this. However, it is wrong to use someone else's work without giving them credit.

GRADING

A 90-100 B 80-89
C 70-79 D 60-69
F otherwise

ADDENDUM

I reserve the right to change the syllabus or content of this course in order to provide a better quality educational product.

CALENDAR

Classes Begin Monday, August 24
Late Registration [1], [2] on myUCF

(ends at 11:59 p.m. on last day) August 24 - 28
Drop Deadline on myUCF *(ends at 11:59 p.m.)* Thursday, August 27
Last Day for Full Refund Thursday, August 27
Add Deadline on myUCF *(ends at 11:59 p.m.)* Friday, August 28
Payment Deadline [1] Friday, September 4
Graduate Thesis/Dissertation Deadline To Request Defense From Advisor Friday, October 9
Graduate Doctoral Dissertation Format Review Deadline Friday, October 9 Academic Advising Weeks October 12 - 23
Grade Forgiveness Deadline on myUCF *(ends at 11:59 p.m.)* Friday, October 16
Withdrawal Deadline *(ends at 11:59 p.m.)* Friday, October 16
Last day to Reinstate Drop for Nonpayment classes *(ends at 4:00 p.m.)* Friday, October 16
Graduate Master's Thesis Format Review Deadline Friday, October 23
Graduate Thesis/Dissertation Defense Deadline Friday, November 6
Spring Textbook Orders Due Friday, November 13
VA Deferral Payment Deadline [1] Friday, November 20
Graduate Thesis/Dissertation Final Submission Deadline Friday, November 20
Classes End; Last Day to Remove Incomplete [3] Monday, December 7
Final Examination Period December 8 - 14
On-campus Housing closes *(noon)* Tuesday, December 15
Grades Due on myUCF *(noon)* Thursday, December 17
Degree Conferral Date Friday, December 18
Commencement December 18 - 19 Grades will be processed as available and will be final at 9 a.m. on myUCF Saturday, December 19

Fall Holidays

Labor Day Monday, September 7
Veteran's Day Wednesday, November 11
Thanksgiving November 26 - 28

FREQUENTLY ASKED QUESTIONS AND ANSWERS:

Note: These are actual questions I've had from students. You will think some of them are funny, some are sad. Nevertheless, I have to post this because I will get questions like these on occasion. I'm posting these to help you preemptively point you to some questions you might have.

Question: "I waited until 11:00PM to upload the assignment and my computer crashed!" OR "I waited until 11:00PM to upload the assignment and WebCT was down! Can I turn my assignment in late? "
Answer: Yes, but you start out with a 75. Sorry, otherwise I have students wanting to turn in an assignment days late.

Question: May I email you about a question about the assignment?
Answer: I would prefer that you post the question to the "Ask the Professor" discussion group. Typically, if a student asks class-related questions, there are several other students who also have the same question.

If it is something of a **personal nature** (that is, only applies to you), then of course, email me.

Question: "Why did you deduct 25% from my grade for not following your naming convention on the assignment, i.e., <first name>.<last name>.<assignment#>.[txt,doc]?
Answer: a) because otherwise I would get 50 assignments named "assignment1.txt", and b) because I told you I would.

Question: I just found out something in your notes, or something you said, that was incorrect. Should I tell you?
Answer: Absolutely! Just make sure you are correct before informing me. I will confirm, but I always want my materials to be up-to-date and accurate. However, things change and I miss things occasionally.

Question: I think you took off points from my assignment when I was correct. Will you regrade it?
Answer: Absolutely! Occasionally I miss things (not the norm though). Of course, if I find something negative that I missed the first time, I will have to deduct points from that.

Question: I'm graduating and I'm failing your course! Can't you just give me a passing grade?
Answer: Of course, in fact, I'm going to give everyone an A just for signing up. A's for everyone! Be real. 95% of my students work hard to learn something and pass this class. If you haven't worked hard, you can only blame yourself. Let this be a lesson. Don't even ask.

Question: "I really blew the first assignment! Do you think I can still pass?"
Answer: It depends on several factors, including how well you do on subsequent assignments. I sometimes discount the first assignment if a student is just learning my expectations, and they do much better of subsequent assignments. If you start out doing well, and go downhill, well that's a different story.

Question: "Which version of Linux is best?"
Answer: It depends. For this class I would suggest a Redhat-like distribution (Redhat, Fedora, or SuSE), or a Debian-based distribution (Debian, Ubuntu, Knoppix, etc).

INSTRUCTOR QUALIFICATIONS

Dr. Philip Craiger, CISSP
Assistant Director for Digital Evidence
National Center for Forensic Science
Assistant Professor
Department of Engineering Technology
College of Engineering and Computer Science
University of Central Florida

Professional Certifications

1. Certified Information System Security Professional (CISSP), 2004
2. SANS GIAC Certified Computer Forensic Analyst (GCFA) 2004

3. EnCase Certified Examiner, 2004, 2006
4. American Society of Crime Labs/Laboratory Accreditation Board (ASCLD/LAB) Certified Inspector, 2004
5. SANS GIAC Certified Security Essentials (GSEC) 2003
6. EC-Council Certified Ethical Hacker (CEH) 2004

Related Professional Publications/Conference Presentations (Digital Forensics/Computer Security)

1. G. Dorn, C. Marberry, S. Conrad, and P. Craiger. Forensic analysis of virtual machines impact on host machine. In G. Peterson and S. Shenoi (Eds.), Advances in Digital Forensics V, Springer, New York. To appear.
2. S. Conrad, C. Rodriguez, C. Marberry, and P. Craiger. Forensic analysis of the Sony Playstation Portable. In G. Peterson and S. Shenoi (Eds.), Advances in Digital Forensics V, Springer, New York. To appear.
3. P. Craiger, Digital Evidence. In H. Bigdoli (Ed.), Handbook of Technology Management. New York: John Wiley & Sons, to appear.
4. P. Craiger, P. Burke, C. Marberry, & M. Pollitt. A virtual digital forensics lab. In I. Ray and S.
5. Shenoi (Eds.), Advances in Digital Forensics IV. Springer, New York, pp. 357-370, 2008.
6. P. Craiger, Training and Education in Digital Forensics. In J. Barbara (Ed.), Handbook of Digital and Multimedia Evidence. Humana Press, pp. 11-22. 2008.
7. P. Craiger, P. Burke, and C. Marberry (to appear). Forensic Examination of Phishing Cases with Free and Open Source Tools. Proceedings of the Anti-Phishing Working Group.
8. P. Craiger, C. Whitcomb, and R. Eaglin. Masters in Digital Forensics. Proceedings of the 41st Annual Hawaii International Conference On System Sciences.
9. P. Craiger and P. Burke, Mac OS X Forensics. In M. Olivier and S. Shenoi (Eds.), Advances in Digital Forensics II, International Federation for Information Processing Working Group 11.9 (Digital Forensics), New York, to appear.
10. P. Burke and P. Craiger, Trace evidence of secure delete programs. In M. Olivier and S. Shenoi (Eds.), Advances in Digital Forensics II. International Federation for Information Processing Working Group 11.9 (Digital Forensics), New York, to appear.
11. P. Craiger, Training and Education in Digital Forensics. In J. Barbara (Ed.), Handbook of Digital and Multimedia Evidence. Humana Press, to appear.
12. P. Craiger, M. Pollitt, C. Marberry, and P. Burke. CD-ROM Burn Attributes Affect Hashes. American Academy of Forensic Science Annual Meeting. San Antonio, TX. February, 2007.
13. C. Whitcomb, P. Craiger, R. Jewell, and M. Pollitt. Primer and Update on Digital Evidence. American Academy of Forensic Science Annual Meeting. San Antonio, TX. February, 2007.

14. P. Craiger, Computer forensics methods and procedures . In H Bigdoli, (Ed), Handbook of Information Security, New York, John Wiley and Sons, 2, pp. 736-755, 2006.

15. P. Craiger, M. Pollitt and J. Swauger, Digital Evidence and law enforcement In H Bigdoli, (Ed), Handbook of Information Security, New York, John Wiley and Sons, 2, pp. 739-777, 2006.

16. P. Craiger, Recovering digital evidence from Linux systems, In S. Shenoi and M. Pollitt (Eds), Advances in Digital Forensics, New York, International Federation of Information Processing Working Group 11.9 (Digital Forensics), pp. 233-243, 2006.

17. P. Craiger, J. Swauger and C. Marberry, Digital evidence obfuscation: recovery techniques. The Proceedings of the International Society for Optical Engineering, pp. 777-888, 2005.

18. P. Craiger, Portable forensics with Linux Annual Meeting of the Nebraska Academy of Sciences, Lincoln, NE, 2004.

19. P. Craiger, et al, An applied course in network forensics Proceedings of the Workshop for Dependable and Secure Systems University of Idaho, Moscow, Idaho, Sept 23-35, 2002.

20. P. Craiger and J. Swauger, Digital forensic software tool validation. In P Kanellis (Ed) Digital Crime and Forensic Science in Cyberspace Idea Group, in press.

21. P. Craiger and P. Burke. Mac Forensics: Mac OS X and the HFS+ File System. Second Annual Conference of the International Federation for Information Processing Working Group 11.9 (Digital Forensics). Feb. 2, 2006, Orlando, FL.

22. P. Burke and P. Craiger Trace evidence of secure delete programs. Second Annual Conference of the International Federation for Information Processing Working Group 11.9 (Digital Forensics). Feb. 2, 2006, Orlando, FL.

23. R. Eaglin and P. Craiger, Data Sharing and the Digital Evidence Markup Language. 1st Annual GJXDM Users Conference, Atlanta, GA. (not peer reviewed), 2005.

24. P. Craiger, Recovering digital evidence from Linux systems, First Annual Conference of the International Association of Information Professionals Working Group 11.9 (Digital Forensics), Orlando, FL, February, 2005.

25. P. Craiger, Digital evidence obfuscation: Recovery techniques Meeting of the International Society for Optical Engineering Orlando, FL, April, 2005.

26. P. Craiger, Portable Linux Forensics, Presentation accepted for the 26th Annual Department of Energy Conference on Computer Security Training Kansas City MO, May, 2004.

27. P. Craiger and S. Webb, Forensics with Linux Presentation for the 8th Annual INFOTEC Conference Omaha, NE, April, 2004.

28. P. Craiger, Network forensics investigative techniques, 25th Annual Department of Energy Conference on Computer Security Training Baltimore MD, April, 2003.

29. S. Webb and P. Craiger, Defensive Battle Stations In Network-Centric Warfare: Rapid-response Computer and Intrusion Forensics Proceedings of the 6th Annual Systems Engineering Conference, San Diego, CA, October, 2003.

30. K. Gubbels and P. Craiger, Honeypots for Defense-in-Depth 25th Annual Department of Energy Conference on Computer Security Training Baltimore MD, April, 2003.

31. P. Craiger, Computer and network forensics Presentation at the 7th Annual INFOTEC Conference Omaha, NE, April, 2003.

32. K. Gubbels and P. Craiger, Defense-in-depth with honeypots Presentation at the 7th Annual INFOTEC Conference Omaha, NE, April, 2003.

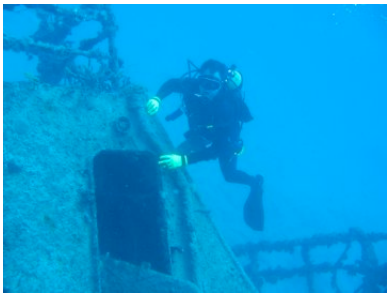
33. P. Craiger, An applied course in network forensics, Paper presented at the Workshop for Dependable and Secure Systems University of Idaho, Moscow, Idaho, Sept 23-35, September, 2002.

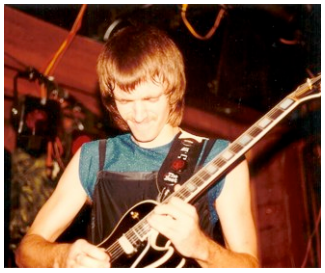
34. P. Craiger, Ubiquitous Security? Presentation at the 6th Annual INFOTEC Conference, April, 2002.

35. S. Whalen and P. Craiger, Attacking and Defending Wireless Networks, Presentation at the 6th Annual INFOTEC Conference, April, 2002.

CET3529 Syllabus Fall 2009

What I do for fun





(Yeah, the last picture is pretty old, but I can still rock.)